UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/425,736	10/22/1999	YUSAKU FUJII	991176	9951

38834 7590 03/20/2007

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	03/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/425,736
Filing Date: October 22, 1999
Appellant(s): FUJII ET AL.

Thomas E. Brown
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/02/2006 and the response to the notice of non-compliant appeal brief filed 12/01/2006 appealing from the Office action mailed 12/02/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: Claims 3-4, 6-11, ~~12,~~ and 14-22 are rejected under 35 USC § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406) and McNair (USP 5,276,444) as applied to claims 1 and 12, and further in view of Gressel (USP 6,311,272).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,035,406	Moussa et al.	03-2000
5,276,444	McNair	01-1994
6,311,272	Gressel	10-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 11 and 22:

These claims recite the limitation "the service providing system" in line 3. Due to the amendments made to claims 1 and 12, a service providing system is no longer previously introduced in the parent claim. Therefore, there is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 5, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moussa et al., United States Patent No. 6,035,406 and further in view of McNair, United States Patent No. 5,276,444

As per claims 1 and 12:

Moussa et al. substantially teach an illegal access discriminating apparatus comprising: a first storing unit for temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authentication (col. 3, lines 24-33); a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication (col. 3, lines 24-33); and a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in second storing unit which were inputted and not previously registered in the past (col. 3, lines 24-33 and col. 4, lines 56-64).

Not explicitly disclosed is a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy

predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value. However, McNair teaches a threshold per biometric sample type that can possibly be used by each individual in order to indicate an attacker in the event of numerous unsuccessful authentication attempts (col. 13, lines 38-68). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Moussa et al. to determine that the numerous unsuccessful authentication attempts are a result of an attacker trying to gain access. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since McNair suggests the feature of only allowing those requesters that reach a certain level of authentication using one type of biometric sample to supply another type of sample up to a certain threshold until all possibilities are exhausted and the requester is either authenticated or locked out from being authenticated in col. 13, lines 38-68.

As per claim 5:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Furthermore, Moussa et al. teaches a person trying to gain access enters a password, then transmits the biometric-password for identification along with the hardware code and identifies the payer using the biometric sample (Fig. 2).

III. Claims 3-4, 6-11, and 14-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moussa et al., United States Patent No. 6,035,406 and McNair, United States Patent No. 5,276,444 as applied to claims 1 and 12 above, and further in view of Gressel, United States Patent No. 6,311,272.

As per claim 3:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach control unit determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of the comparing and collating unit. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-34). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow unauthorized entries to be halted.

As per claim 4:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest,

the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair, because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 6:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach the inputted organic information and the organic information which was inputted in the past coincide, the control unit detects a combination in which the organic information coincides and the ID information differs, and when the number, the control unit determines that there is the authentication demand by the illegal access person. Gressel teaches a false rejection rate rejects a percentage of individuals when the meeting of the two (false acceptance rate and false rejection rate) nears the threshold (col. 10, lines 5-23). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow the attempted user to be authenticated.

As per claim 7:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic

information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-5). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 8:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card, the original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). 11: would have been

obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 9:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach the storing unit stores a telephone number serving as a transmitting source and a terminal position such as a network address or the like together with the ID information and organic information which were inputted in the past. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and passwords. (col. 11, lines 47-57). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus.

As per claim 10:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and

allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

As per claim 11:

Moussa et al. and McNair substantially teach the system/method as applied to claim 1 above. Moussa et al. and McNair fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an administrator of the service providing system of a result of the discrimination. Gressel teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

As per claim 14:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a control step, it is determined that there is the authentication demand by the illegal access person in the case where

the ID information does not coincide and the organic information does not coincide on the basis of the output in the comparing and collating step. Gressel teaches that 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant. (col. 10, lines 48-54) It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 15:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach telephone number serving as a transmitting source, a terminal position such as a network address, and an input time in correspondence to the ID information and organic information which were inputted in the past are stored and in the control step, it is determined that there is the authentication demand by the illegal access person in the case where the comparison result in the comparing and collating step between the inputted from a same terminal position within a predetermined time indicates dissidence. Gressel teaches secret keys and random numbers are internally generated in smart cards and security application modules in terminal devices. Biometric data in a secure system is equivalent to pins and passwords. (col. 11, lines 47-62). An original template resides in the terminal while a threshold value is in a user's smart card (col. 12, lines 46-51). 3% of the population would be rejected regardless of the value of the threshold. Human intervention then becomes necessary to process the applicant (col. 10, lines 48-54). It would have been

obvious to combine Gressel's teachings to Moussa et al. and McNair to designate a personal ID as telephone numbers and biometric data to increase the security of the apparatus, to store the information to use for authentication, and because of the need to resolve the authentication of applicants who qualify for access with a valid threshold value, but not qualifying organic information.

As per claim 16:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach past ID information has a serial number for the inputted ID information or not is discriminated and, when it is determined that the past ID information has the serial number, i1: is determined that there is the authentication demand by the illegal access person at a predetermined designated number of times. Gressel teaches a fingerprint scan is used in a biotest scan, the threshold value has little effect on the test, and an illegal access person has a limited number of tries because of their fear of being caught (col. 10, lines 40-47). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because a biotest scan would deter unauthorized access attempts and minimize the authentication systems use of the processor.

As per claim 17:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach the inputted organic information and the organic information, which was inputted in the past coincide, a combination in which the organic information coincides and the ID information differs is detected, and

when the number of the combinations reaches a predetermined number, it is determined that there is the authentication demand by the illegal access person. Gressel teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized (col. 10, lines 26-47). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow unauthorized entries to be halted.

As per claim 18:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence and an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained and generating a signal indicative of dissidence of the organic information in the case where a value less than the predetermined coincidence degree is obtained. Gressel teaches a percentage of the population would be rejected and the guards would be signaled (col. 10, lines 48-54). Also, Gressel teaches a false acceptance rate and false rejection rate (col. 9, lines 50-67) and upon comparison with the threshold value, a large subgroup would be allowed entry (col. 9, lines 50-67 and col. 10, lines 1-5). It would have been obvious to combine Gressel's

teachings to Moussa et al. and McNair because it would allow personal information to be used in records for authorization with a specific individual.

As per claim 19:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest, the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 20:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach a timer unit for measuring a time and wherein the ID information and organic information, which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by the timer unit are erased and excluded from targets of the comparison and collation. Gressel teaches upon successful completion of the biotest,

the user's biometric features are encoded into the smart card. The original template threshold value is a parameter, which is typically determined by the system application owner, depending on the application. (col. 12, lines 42-48) The ID module detects a payee or payer by conducting a re-registration check (col., 9, lines 33-41). It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins. The thresholds and templates are only read from the user.

As per claim 21:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach an authentication demand terminal address recording unit for recording the number of times of authentication demand every terminal address and the same terminal access detecting unit for detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to the authentication demand terminal address, activating the comparing and collating unit and the control unit and allowing an illegal access to be discriminated. Gressel teaches the use of an original template threshold value, which sets values that are larger than the user's smart card threshold value. This threshold value is incremented appropriately and thus records the demands on the authentication process. Gressel teaches the use of a biotest to compare fingerprints where only 3 percent of the population would be rejected (col. 12, lines 45-51). It would have been obvious to combine Gressel's teachings to Moussa et

al. and McNair because preliminary screening of users reduces fraudulent access to the authentication system, thus reducing processor time.

As per claim 22:

Moussa et al. and McNair substantially teach the system/method as applied to claim 12 above. Moussa et al. and McNair fail to teach that when it is determined that there is the authentication demand by the illegal access person, the control unit automatically notifies an administrator of the service providing system of a result of the discrimination. Gressel teaches a rejection results in the further processing of the applicant by a guard (col. 10, lines 48-54). The guard is comparable to an administrator. It would have been obvious to combine Gressel's teachings to Moussa et al. and McNair because the use of an administrator's intervention would facilitate the accuracy of the authentication process.

(10) Response to Argument

Regarding Claims 11 and 22, 35 USC 112, 2nd paragraph rejection:

Appellant contends that claims 11 and 22 as amended in the amendment dated April 3, 2006 resolve the antecedent basis issue concerning the phrase, "a service providing system." Examiner agrees and therefore withdraws the 35 USC 112, second paragraph rejection with regards to these claims.

Regarding Claims 1 and 12, 35 USC 103(a) Rejections:

Appellant contends, "The term 'fingerprint' referred to in the present invention concerns a human fingerprint ('origin in formation' recited in claim 1 of the present invention). The fingerprint in the cited reference means a hash value1 (*1) of a certain data, as described in col. 4, lines 50-54." Appellant further states that the cited portion of Moussa et al., i.e. col. 6, lines 64-67, "This expresses that a new 'fingerprint' is prepared from a data block 132. This means that a new fingerprint (hash value) is created from data written in the data block 132. It is not correct to interpret this fingerprint as being a human fingerprint which is invariable all the life." Examiner would first like to point out that the independent claims 1 and 12 make no reference to a fingerprint, as the claim language only calls for "organic information." Furthermore, Examiner would like to point out that in the Appellant's disclosure (page 17, lines 23-25), the various types of organic information are disclosed as follow: "*However, organic information such as iris, voiceprint, retina blood vessel distribution, **signature**, or the like other than the fingerprint can be used.*" Moussa et al. teach the use of a handwritten signature (which is a form of biometric information) used in combination with other identification information (see below for details) in order to authenticate a user to a system in col. 5, lines 28-40: "*At a step 226, the login service performs such other authentication as desired*"..."*however, in alternative embodiments, the login server 140 may perform signature verification for the user in the step 226. The step 226 may be performed using the following technique: The login server 140 maintains a signature verification template T, using techniques such as described in detail in the Incorporated Disclosures.* ***At a***

sub-step 226(a), the login server 140 receives a signature from the user (using a signature receiving device such as a writing tablet)."

Appellant further contends that "Moussa is also simply not concerned with storing pairs of ID information and organic information which were inputted by arbitrary users **within predetermined time**." Examiner respectfully disagrees. In reference to the argued limitation, Moussa et al. teach that in order for the user to gain access to the system, he/she must first be authenticated using **at least two-factor** security authentication: "*The invention provides a method and system for simultaneously authenticating a user using two or more factors, such as using both a password and a physical token,* ***or using a password, a physical token, and biometric information***" in col. 2, lines 5-8. Specifically, Moussa et al. teach that the user enters in a user name in order to begin the authentication process: "*At step 221, the enters their associated user name. In a preferred embodiment, the* ***user name is a unique value which describes the user****, and may comprise the user's actual name, but may also comprise a mnemonic name such as the user's initials. User names are known in the art of computer security. The login service receives the user name and begins execution on the processor 110*" in col. 3, lines 61-67. Furthermore, Moussa then teaches that the user must also enter in a password in addition to his/her user name, where the password entered is used to obtain the password which the operating system associates with the user, i.e. ID information: "*At a step 222,* ***the user enters a first password Q****. The login service 140 receives the first password Q. The first password Q is not the password P which the operating system 150 associates with the user name,*

and cannot be used to gain access to the processor 110 using the operating system 150. ***The login service 140 uses the physical token 131 to determine the password P in response to the first password Q, and thereafter authenticated the password P using the operating system 150****, thus authenticating both that the physical token 131 is present and that the first password Q was correctly entered*" in col. 4, lines 1-12. Finally, in reference to the user's ID information, Examiner would like to point out Moussa et al. proceed to discuss the details of how the password information (and as will be shown later, also the signature information) will be used as the ID information: "*At as step 223, the login service 140 determines a set of index values Ni in response to the first password Q. In a preferred embodiment,* ***one index value Ni is determined for each character of the password P plus one additional index value N0,*** *and the password P is selected to have a maximum length permitted by operating system 150"..."At a sub-step 223(b),* ***each selected combination from the sub-step 223(a) [where 223(a) derives the different combinations using the letters of password] is converted to an integer value****"..."At a sub-step 223(c), each integer value is input into a pseudorandom number generator..."* in col. 4, lines 13-38. The previous information is used in identifying/authenticating the user. The Examiner also directs Appellants attention to the portion of Moussa et al. which discloses an alternate embodiment to use a biometric signature in addition to the preferred embodiment, "***At a step 226, the login service performs such other authentication as desired****. In a preferred embodiment, there is no such other authentication;* ***however, in alternative embodiments, the login server 140 may perform signature verification for the user***

in the step 226. *The step 226 may be performed using the following technique: The login server 140 maintains a signature verification template T, using techniques such as described in detail in the Incorporated Disclosures.* ***At a sub-step 226(a), the login server 140 receives a signature from the user (using a signature receiving device such as a writing tablet***" in col. 5, lines 28-40. Furthermore, Moussa et al. teach that once the required authentication data is received/authenticated and various hash values are calculated based on the submitted authentication information, the new values for the authentication number (i.e. for that specific login session) and the data block are eventually stored in a database: *"****At a flow point 230, the user has been successfully authenticated.*** *The method 200 for two-factor security authentication continues with a sequence of further flow points and steps. At step 241, the login service* ***generates a new data block 132*** *for the physical token 131. In a preferred embodiment, the step 241 is performed using the following technique: The login service 140* ***generates a new authentication number N****"..."The login service 140 recomputes the indexing sums (Ni+N*) using the new authentication number N*. At* ***step 242, the login service 140 writes the new data block 132 onto the physical token 131.*** *In a preferred embodiment, the* ***step 242 is performed using the following technique:*** *The login service 140 writes the random value into the data block 132 on the physical token 131.* ***The login service 140 writes each character Pi of the password P into the data block 132 at the location specified by the corresponding indexing sum (N1+N*).*** *The login service 140 writes the new authentication number N* into the data block 132 at the location specified by the additional index value N0, thus, at location (2000 + N0)*"

in col. 6, lines 59. The previously cited portion of Moussa et al. is used to establish that the authentication information, in this case the password (or each character of the password Pi), is written to the newly calculated index locations in the physical token, as well as in the second storage: "*At a step 243, the login service 140 stores new values in its* ***authentication database 141***" in col. 6, lines 60-61. In reference to the organic information, the same arguments as presented by the Examiner in reference to the ID information apply (i.e. the password P in combination with the user name information previously discussed), as Moussa et al. disclose that a signature may be treated in the same manner as the password as described above: "***The signature verification template T may be distributed in the data block 132 using a technique similar to the techniques described herein for distribution of the password P in the data block 132***" in col. 5, lines 60-64. Finally, in reference to the phrase "within predetermined time," Examiner would like to point out that the phrase "predetermined time" is extremely broad and is therefore broadly interpreted according to MPEP 2111. Therefore, predetermined time has been interpreted, with reference to Moussa et al., to encompass the predetermined time for which the system continuously accepts authentication data from various users, i.e. for the duration of the time that the system is in use: "*The login service 140 maintains an authentication database 141, in which it associates an authentication fingerprint F and an authentication number N, for* ***each particular user for each particular login session***" in col. 3, lines 24-26. The Examiner would like to clarify that in the above-cited portion the "fingerprint" derived is a hash value which is derived based on the authentication data (which in the presently

cited reference includes a password and a hand-written signature) provided in the data block of the physical token.

Applicants further contend that "Examiner has failed to appreciate that McNair is simply not concerned with counting the number of comparing-collating results which **satisfy predetermined conditions** and judging authentication demand as the one by an attacker **if the counted number exceeds a predetermined value**." Examiner respectfully disagrees. McNair teaches a "try-again" threshold which is used to allow users who meet a specified pre-determined range when submitting the authentication data that was requested from them to try to meet an alternate authentication challenge: "***For each type of authentication information there may be a 'try again threshold*** *which when reached, during an iteration of step 825, indicates that the received authentication information yields an authentication that is close to the desired level but the authentication remains as yet uncertain"...****If the 'try again' threshold is reached, access should not be granted to the desired level but the requester may be allowed to supply a different form of authentication information to obtain access.*** *Therefore, if the test result in subsequent iterations of step 825 is that access decision unit 208 of SCP 134-1 remains unsure as to whether access should be allowed at the level requested, the test result in 825 is DON'T KNOW and* ***control is passed to conditional branch point 835***" in col. 13, lines 38-56. McNair further teaches that a user can only "try again" to the point of number of different types of authentication information that exist (in the user profile) for challenging the user with. Once there is no more authentication information to test the user's response against, the user exceeds

the limit defined by that predetermined value and is not authorized to try again and is judged as being an attacker: "***Conditional branch point 835 tests to determine if there remains authentication information that can be obtained from the access requester, as specified in the profile,*** *or alternatively if additional authentication features can be extracted from the information which the requester has already supplied*" in col. 10, lines 14-20 and also see McNair, **Fig. 6**, element **835** and follow the "***No***" situation which continues on to **Fig. 7** which leads to element **817 "*Connection is Refused*"** and then in element 819 where the "*Transaction is Journalized.*"

Regarding Claims 3 and 14, 35 USC 103(a) Rejections:

Appellant contends that Moussa et al., McNair and Gressel fail to disclose "a control unit [that] determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of said comparing and collating unit." Examiner agrees that Moussa et al. and McNair fail to disclose this feature, however respectfully disagrees that Gressel fails to suggest this feature. Moussa et al. and McNair et al. substantially teach claims 1 and 12 based on the arguments above. Moussa further teaches the use of two or more factors in an authentication scheme in order to result in stronger authentication (the more factors the stronger the likelihood that an unauthorized user will not gain access to the system): "*The invention provides a method and system for simultaneously authenticating a user using two or more factors,*

such as using both a password and a physical token, or using a password, a physical token, and biometric information" in col. 2, lines 5-8. However, since Moussa et al. and McNair failed to teach the features claimed in these dependent claims, Gressel was introduced to remedy the shortcomings of the Moussa et al. and McNair combination (with regards to claims 3 and 14). Gressel teaches that the PIN and biometric data are compared with the stored data for authentication, as well as that when these two forms of authentication data are supplied they must both be satisfied in order for the user to gain access to the system: "*The smart card now decrypts the data from the terminal and* ***can compute the proximity of the biotest to the reference templates, compare the PIN number to the number stored in its memory****, update the last reference template*" in col. 15, lines 62-65. Thus, when two factor authentication is used, if one of the two factors is not verified, the system will not grant storage of the new biometric template, as it will assume that and attack is being launched: See Gressel, **Fig. 8A**, element **700** "***PIN/PASSWORD & BIOMETRIC***" following arrows to both element **710** "***SMARTCARD DECIDES PASSWORD GOOD?***" and 720 "*COMPARE BIOTEST TO REFERENCE (FIG.5)*" to **730** "***BIOCHECK SUCCESSFUL?***" and finally, following "NO" to element **740 "REFUSE ABORT."** Thus, Fig. 8A as described shows that if either the PIN/PASSWORD or the BIOMETRIC information are not good, access is refused and the process is aborted, however when both items are good, then the process may continue.

Regarding Claims 4 and 15, 35 USC 103(a) Rejections:

Appellant contends that Moussa et al., McNair and Gressel fail to disclose "said control unit determines that there is the authentication demand by the illegal access person in the case where the comparison result by said comparing and collating unity between the inputted ID information and the past ID information inputted from a same terminal position within a predetermined time indicates dissidence." Examiner agrees that Moussa et al. and McNair fail to disclose this feature, however respectfully disagrees that Gressel fails to suggest this feature. Moussa et al. and McNair et al. substantially teach claims 1 and 12 based on the arguments above. Furthermore, Moussa et al. teach that if there is an unsuccessful login attempt that there may be a time delay before allowing a user to try again: "*In a preferred embodiment, the login server 140 displays the fact of an unsuccessful authentication and allows the user to try again at the flow point 210* ***after a time delay***" in col. 6, lines 22-24. However, since Moussa et al. and McNair failed to teach the features claimed in these dependent claims, Gressel was introduced to remedy the shortcomings of the Moussa et al. and McNair combination (with regards to claims 4 and 15). Gressel suggests that proximities between attributes of the last revised template and the present measured value are monitored, as well as that the risk management feature in the card can determine a maximum number of biotest rejections before locking an application so an unauthorized user cannot gain access: "***It is preferable to compare the last measurement both to the last updated template 390 and to either the original enrollment template or to the revised reference template 360.*** *Typically, the last*

updated template 380 has a value reasonable close to the present measured value and the revised reference template 370 is typically an enhanced version of the original template 310"...."The last date the template was revised, as stored in field 400, can serve as a measure of quality of the last revised template. ***Typically, this can be read by a terminal, and have an effect on a threshold value. The biocounter 410 is incremented at every biotest.*** *Typically, as in FIGS. 5A-5B, this can define when the original reference template 310 can be replaced by a revised template 360which is typically assumed to be more accurate.* ***Risk management in the card may typically determine a maximum number of biotest rejections before locking an application, prior to a reenrolling procedure***" in col. 131, lines 1-29. Furthermore, Gressel suggests that these events all occur on the same terminal which archives the data in regards to the transactions performed: "*In the general scheme depicted in FIG. 6, mutual terminal and smart card transmissions are executed, authenticated, and responsibly accepted, without any data which identifies the smart card, the smart card user, or the* ***transaction data*** *appearing in the clear on the interface between the smart card and the terminal."..."As terminal data is processed in the terminal SAM, a strategy can be determined by the system integrator as to* ***which data can be archived in the terminal****, and which data can be encrypted for transmission to a transaction acquirer and which can be sent in the clear*" in col. 14, lines 54-67. Thus, Gressel suggests that keeping track of various transactions occurring on a terminal can help in detecting attack attempts made from the same terminal.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Nadia Khoshnoodi

Nadia Khoshnoodi

Conferees

Eddie Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

Emmanuel Moise

E. Moise